ELEKTRONISCHE IDENTIFIZIERUNG UND VERTRAUENSDIENSTE

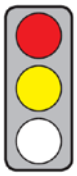
cep**Analyse** Nr. 31/2012 vom 30.07.2012

Centrum für Europäische Politik

KERNPUNKTE

Ziel der Verordnung: Die Kommission will mit ihrem Vorschlag das Vertrauen in elektronische Transaktionen im Binnenmarkt stärken.

Betroffene: Bürger, Unternehmen, Behörden.



Pro: (1) Die grenzüberschreitende Anerkennung und Akzeptierung elektronischer Identifizierungsmittel kann Bürokratie- und Transaktionskosten senken.

(2) Die Vorschriften zur Sicherheit elektronischer Signaturen verbessern die Interoperabilität, was grenzüberschreitende Aktivitäten erleichtert.

Contra: (1) Der Verzicht auf eine Prüfung, ob die Identifizierungssysteme den Vorschriften entsprechen, erleichtert den Missbrauch und gefährdet die Sicherheit von Personendaten.

(2) Die Aufsichtsregeln für Anbieter der besonders sensiblen „qualifizierten Vertrauensdienste" sind unpräzise und inkonsistent.

INHALT

Titel

Vorschlag KOM(2012) 238 vom 4. Juni 2012 für eine **Verordnung** des Europäischen Parlaments und des Rates über die **elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt**

Kurzdarstellung

- **Hintergrund und Ziele**
  - Die Verordnung erweitert die bisherigen Vorschriften zum Vertrauensdienst elektronische Signatur (Richtlinie 1999/93/EG) und ergänzt sie um neue Vorschriften über die elektronische Identifizierung und zusätzliche Vertrauensdienste.
  - Ziel der Kommission ist es u.a. (Begründung S. 2),
    - das Vertrauen in elektronische Transaktionen in der EU zu stärken,
    - die Sicherheit elektronischer Transaktionen zu gewährleisten,
    - die Interoperabilität elektronischer Identifizierungssysteme zu verbessern.
- **Begriffe**
  - „Elektronische Identifizierung" ist der Prozess der Identifizierung einer Person durch elektronische Daten (Art. 3 Abs. 1), etwa durch elektronische Personalausweise.
  - „Vertrauensdienste" und „qualifizierte Vertrauensdienste"
    - „Vertrauensdienste" sind elektronische Dienste zur „Erstellung, Überprüfung, Validierung, Handhabung und Bewahrung" von elektronischen Signaturen, Siegeln, Zeitstempeln, Dokumenten, Zustelldiensten und Zertifikaten sowie von Verfahren zur Prüfung, ob eine Webseite von ihrem Inhaber stammt (Authentifizierung) (Art. 3 Abs. 12).
    - „Qualifizierte Vertrauensdienste" sind Vertrauensdienste, die den Anforderungen der vorliegenden Verordnung genügen (Art. 3 Abs. 13).
      Zu ihnen zählen u.a. „qualifizierte Zertifikate". Diese dienen der Verknüpfung von elektronischen Signaturen, Siegeln und Webseiten mit einer Person (Art. 3 Abs. 10 i.V.m. Abs. 11, 24 und 30).
  - Elektronische Signaturen
    - „Einfache elektronische Signaturen" sind elektronische Daten, die zum Unterzeichnen verwendet werden (Art. 3 Abs. 6), z.B. eingescannte Unterschriften.
    - „Fortgeschrittene elektronische Signaturen" sind elektronische Signaturen, die u.a. (Art. 3 Abs. 7)
      - einem Unterzeichner eindeutig zugeordnet sind,
      - dessen Identifizierung ermöglichen und
      - mit elektronischen Signaturerstellungsdaten erstellt werden, die nur der Unterzeichner verwenden kann.
    - „Qualifizierte elektronische Signaturen" sind fortgeschrittene elektronische Signaturen, die von einer „qualifizierten elektronischen Signaturerstellungseinheit" erstellt wurden und auf einem „qualifizierten Zertifikat für elektronische Signaturen" beruhen (Art. 3 Abs. 8).
      - „Qualifizierte elektronische Signaturerstellungseinheiten" sind „Soft-oder Hardware", die die Anforderungen des Anhangs II der Verordnung erfüllt (Art. 3 Abs. 17 und 18).
      - „Qualifizierte Zertifikate für elektronische Signaturen" müssen die Anforderungen des Anhangs I der Verordnung erfüllen (Art. 3 Abs. 11).
- **Anwendungsbereich**
  - Die Verordnung regelt (Art. 2 Abs. 1)
    - die elektronische Identifizierung, die von den Mitgliedstaaten, in deren Namen oder unter deren Verantwortung bereitgestellt wird, und

Autoren: Anne-Kathrin Baran und Philipp Eckhardt | baran@cep.eu
CEP | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-105 | www.cep.eu

- die Tätigkeit von in der EU niedergelassenen Anbietern von Vertrauensdiensten; ausgenommen sind Vertrauensdienste, die innerhalb geschlossener Gruppen auf Basis „freiwilliger privatrechtlicher Vereinbarungen“ angeboten werden (Art. 2 Abs. 2); dazu zählen z.B. spezielle Signatursysteme für die Kommunikation zwischen Anwälten und Gerichten.

- **Elektronische Identifizierung (electronic identification, e-ID) und Notifizierung**
  - Die Mitgliedstaaten müssen in einem anderen Mitgliedstaat ausgestellte elektronische Identifizierungsmittel, z.B. elektronische Personalausweise, anerkennen und akzeptieren. Voraussetzung dafür ist, dass dieser Staat das elektronische Identifizierungssystem, welches er zur Ausstellung der Identifizierungsmittel verwendet, bei der Kommission notifiziert hat (Art. 5).
  - Die Mitgliedstaaten können elektronische Identifizierungssysteme notifizieren, wenn sie (Art. 6 Abs. 1)
    - die elektronischen Identifizierungsmittel ausstellen oder ausstellen lassen,
    - diese elektronischen Identifizierungsmittel selbst akzeptieren,
    - sicherstellen, dass die zur Identifizierung erforderlichen Daten „eindeutig“ einer Person zugeordnet sind,
    - es Dritten jederzeit und kostenlos ermöglichen, die Gültigkeit der elektronischen Identifizierung online zu prüfen (Authentifizierung), und
    - für die Einhaltung der beiden letzten Anforderungen haften.
  - Die Kommission erstellt und veröffentlicht eine Liste aller notifizierten Identifizierungssysteme (Art. 7 Abs. 2).
  - Die Mitgliedstaaten arbeiten zusammen, um die Interoperabilität elektronischer Identifizierungsmittel zu gewährleisten, die im Rahmen eines notifizierten Identifizierungssystems ausgestellt wurden (Art. 8 Abs. 1).
  - Die Kommission kann
    - in Durchführungsrechtsakten „Einzelheiten, Form und Verfahren“ der Notifizierung festlegen (Art. 7 Abs. 4),
    - in delegierten Rechtsakten „technische Mindestanforderungen“ festlegen, um die grenzüberschreitende Interoperabilität zu fördern (Art. 8 Abs. 3).
- **Vertrauensdienste: Vorschriften für alle Anbieter von Vertrauensdiensten**
  - Die Mitgliedstaaten benennen eine Aufsichtsstelle für Anbieter von Vertrauensdiensten (Art. 13 Abs. 1 und 2).
  - Diese Anbieter müssen „technische und organisatorische Maßnahmen“ ergreifen, um ein „angemessenes Sicherheitsniveau“ sicherzustellen (Art. 15 Abs. 1 UAbs. 1). „Erhebliche“ Sicherheitsverletzungen müssen sie „unverzüglich“, „falls möglich“ innerhalb von 24 Stunden nach Kenntniserlangung der Aufsichtsstelle und „anderen einschlägigen Dritten wie Datenschutzbehörden“ melden (Art. 15 Abs. 2 UAbs. 1).
  - Verletzen Anbieter von Vertrauensdiensten die allgemeinen Sicherheitsanforderungen, haften sie für alle „unmittelbaren Schäden“ (Art. 15). Dabei ist eine Beweislastumkehr vorgesehen: Die Anbieter müssen beweisen, dass sie nicht fahrlässig gehandelt haben. (Art. 9)
- **Vertrauensdienste: Vorschriften für Anbieter von qualifizierten Vertrauensdiensten**
  - Für Anbieter von qualifizierten Vertrauensdiensten gelten zusätzliche Sicherheitsanforderungen (Art. 19).
  - Insbesondere müssen sie die Identität einer Person überprüfen, für die sie ein „qualifiziertes Zertifikat“ (s.o.) ausstellen (Art. 19 Abs. 1 UAbs. 1, Art. 3 Abs. 10). Die Überprüfung erfolgt durch (Art. 19 Abs. 1 UAbs. 2 lit. a und b)
    - einmaliges persönliches Erscheinen der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person oder
    - aus der Ferne durch ein elektronisches Identifizierungsmittel, das einem notifizierten elektronischen Identifizierungssystem unterliegt und bei dessen Ausstellung die Identität des Inhabers überprüft wurde.
  - Anbieter dürfen einen qualifizierten Vertrauensdienst erbringen, sobald sie der Aufsichtsstelle ihre Absicht sowie den Bericht einer „anerkannten unabhängigen Stelle“ übermittelt haben, der bestätigt, dass der Anbieter die Anforderungen der Verordnung erfüllt. Dieser Bericht muss jedes Jahr erneuert werden. (Art. 16 Abs. 1 i.V.m. 17 Abs. 1)
  - Nachdem die Aufsichtsstelle überprüft hat, dass Anbieter und deren Vertrauensdienste die Voraussetzungen der Verordnung erfüllen, führt sie diese Anbieter auf einer „Vertrauensliste“ (Art. 17 Abs. 3). Bei Verstößen gegen die Verordnung können sie aus dieser gestrichen werden. (Art. 16 Abs. 4).
  - Erfüllen die Anbieter von qualifizierten Vertrauensdiensten die allgemeinen und zusätzlichen Anforderungen der Verordnung nicht, haften sie für alle „unmittelbaren Schäden“. Dabei ist eine Beweislastumkehr vorgesehen: Die Anbieter müssen beweisen, dass sie nicht fahrlässig gehandelt haben. (Art. 9)
- **Elektronische Signaturen (eSignatures)**
  - Qualifizierte elektronische Signaturen können handschriftliche Unterschriften ersetzen (Art. 20 Abs. 2). Alle Mitgliedstaaten müssen sie anerkennen und akzeptieren (Art. 20 Abs. 3).
  - Elektronische Signaturen dürfen nicht allein wegen ihrer elektronischen Form als Beweismittel in Gerichtsverfahren ausgeschlossen werden. (Art. 20 Abs. 1).
  - Die Mitgliedstaaten dürfen für den grenzüberschreitenden Zugang zu Online-Diensten öffentlicher Stellen keinen höheren Sicherheitsstandard als den der qualifizierten elektronischen Signatur verlangen (Art. 20 Abs. 5).

– Verlangt ein Mitgliedstaat einen niedrigeren Sicherheitsstandard, so muss er alle elektronischen Signaturen anerkennen und akzeptieren, die zumindest diesen Standard erfüllen. Die Kommission kann durch delegierte Rechtsakte festlegen, welche elektronischen Signaturen im Falle technischer Unterschiede, die Voraussetzungen welcher Sicherheitskategorie – einfach, fortgeschritten, qualifiziert – erfüllen. (Art. 20 Abs. 4 und 6)

Änderung zum Status quo

- Neu eingeführt werden die Vorschriften zur elektronischen Identifizierung und zu den zusätzlichen Vertrauensdiensten.
- Die bereits bestehenden Vorschriften zur elektronischen Signatur werden erweitert um Regeln zur Höhe des Sicherheitsstandards von elektronischen Signaturen.

Subsidiaritätsbegründung der Kommission

Laut Kommission erfordert der „transnationale Charakter" elektronischer Identifizierung und elektronischer Vertrauensdienste EU-Handeln.

Politischer Kontext

In der Mitteilung „Eine digitale Agenda für Europa" [KOM(2010) 245; s. CEP-Analyse] kündigte die Kommission die Überarbeitung der Richtlinie über elektronische Signaturen (1999/93/EG) und einen Vorschlag zur gegenseitigen Anerkennung der elektronischen Identifizierung und Authentifizierung an. Im Rahmen des STORK-Projektes der EU arbeiten zehn Mitgliedstaaten daran, die Interoperabilität elektronischer Ausweise zu ermöglichen.

Stand der Gesetzgebung

04.06.12	Annahme durch Kommission
Offen	Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

Politische Einflussmöglichkeiten

Federführende Generaldirektion:	GD für Kommunikationsnetze, Inhalte und Technologien
Ausschüsse des Europäischen Parlaments:	Industrie, Forschung und Energie (federführend), Berichterstatterin: Marita Ulvskog (S&D-Fraktion, SE); Wirtschaft und Währung; Binnenmarkt und Verbraucherschutz; Recht; Bürgerliche Freiheiten, Justiz und Inneres
Ausschüsse des Deutschen Bundestags:	Wirtschaft und Technologie (federführend); Angelegenheiten der EU; Inneres; Recht
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch Mehrheit der Mitgliedstaaten und mit 255 von 345 Stimmen; Deutschland: 29 Stimmen)

Formalien

Kompetenznorm:	Art. 114 AEUV
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

BEWERTUNG

Ökonomische Folgenabschätzung

Elektronische Identifizierung und Vertrauensdienste werden sich nur dann durchsetzen, wenn es dafür gewinnversprechende Geschäftsmodelle gibt. Wesentliche Hemmnisse dafür sind heute die fehlenden Anwendungsmöglichkeiten, hohe Kosten, Sicherheitsbedenken und regulatorische Unsicherheit. Die Verordnung trägt zu einem Abbau der regulatorischen Unsicherheit bei und stärkt daher den digitalen Binnenmarkt.

Elektronische Identifizierung: Die Anerkennung und Akzeptierung notifizierter elektronischer Identifizierungsmittel anderer Mitgliedstaaten **kann Bürokratie- und Transaktionskosten reduzieren.** Sie ermöglicht eine schnellere Abwicklung von Anliegen mit Behörden und Unternehmen in anderen Mitgliedstaaten, die eine elektronische Identifizierung verlangen. Damit steigen auch Anreize für Unternehmen, grenzüberschreitend tätig zu werden, sich z.B. auf eine Ausschreibung in einem anderen Mitgliedstaat zu bewerben.

Problematisch ist, dass nicht von unabhängiger Seite **kontrolliert wird, ob die notifizierten Identifizierungssysteme** tatsächlich **die in der Verordnung gestellten Anforderungen erfüllen und die Systeme hinreichend hohen Mindestsicherheits- und Datenschutzanforderungen genügen.** Gleichwohl müssen andere Mitgliedstaaten die Identifizierungsmittel dieser Systeme anerkennen und akzeptieren. **Dies vereinfacht Missbrauch**, gefährdet das Vertrauen der Nutzer in die Identifizierungsmittel **und stellt die Sicherheit sensibler Personendaten in Frage. Die** vorgesehene **Haftung der Mitgliedstaaten** mildert dies zwar, **reicht** aber **nicht aus.** Die Notifizierung sollte daher nur nach unabhängiger Prüfung, notfalls auch durch die Kommission, erfolgen können.

Die Interoperabilität der Identifizierungsmittel ist Grundvoraussetzung für die gegenseitige Anerkennung und Akzeptierung und damit für die Funktionsfähigkeit der elektronischen Identifizierung. Fehlende Interoperabilität führt dazu, dass Mitgliedstaaten, die ein notifiziertes ausländisches Identifizierungsmittel anzuerkennen

und zu akzeptieren haben, dafür ihre eigenen Identifizierungssysteme technisch anpassen müssen. Die Interoperabilität hätte daher geregelt werden müssen, bevor eine gegenseitige Anerkennung und Akzeptierung vorgeschrieben wird. Unbeschadet dieser Kritik ist derzeit überhaupt fraglich, inwieweit die Vorschriften zur elektronischen Identifizierung in der näheren Zukunft ihre volle Wirkung entfalten können. Denn erstens verfügen einige Mitgliedstaaten über keine elektronischen Identifikationssysteme, zweitens ist die Notifizierung für die Mitgliedstaaten freiwillig und drittens sind bisher kaum Anwendungen verfügbar.

Vertrauensdienste: Dass die Anbieter von Vertrauensdiensten (ob qualifiziert oder nicht) bei Sicherheitsverletzungen für unmittelbare Schäden haften, stärkt die Rechtssicherheit für die Nutzer und schafft damit Vertrauen in die Vertrauensdienste, gerade auch im grenzüberschreitenden Dienstleistungsverkehr.

Die Aufsichtsvorschriften für die Anbieter der – besonders sensiblen – qualifizierten Vertrauensdienste sind unpräzise und inkonsistent. So kann ein Anbieter auf der „Vertrauensliste" stehen, obgleich er die Anforderungen der Verordnung nicht länger erfüllt und damit seinen Status als qualifizierter Anbieter verloren hat. Auch kann ein qualifizierter Anbieter mit der Erbringung qualifizierter Vertrauensdienste beginnen, ohne dass die Aufsicht geprüft hat, ob er die Anforderungen der Verordnung erfüllt, da ein Zulassungsverfahren fehlt. Hier besteht dringender Klarstellungsbedarf, um die Sicherheit zu gewährleisten. Schon die unkonkreten Aufsichtsregelungen der bisherigen Signatur-Richtlinie haben zu einem Vertrauensverlust beigetragen.

Die Aufnahme weiterer Vertrauensdienste – Zeitstempel, Siegel, Dokumente, Zustelldienste, Zertifikate – in die Regulierung ist sachgerecht. Denn es gibt für diese Vertrauensdienste bisher nur nationale, häufig divergierende rechtliche und technische Regelungen, was grenzüberschreitende Aktivitäten der Anbieter behindert. Zudem herrscht Unsicherheit bei Nutzern wie Anbietern über die Rechtsgültigkeit der Dienste im EU-Ausland, was das Vertrauen und die Attraktivität der Dienste schwächt.

Elektronische Signatur: Die Umsetzung der bisherigen Signatur-Richtlinie in nationales Recht hat zu unterschiedlichen nationalen Qualitäts- und Sicherheitsniveaus für die elektronischen Signatur geführt. Ergebnis waren national geprägte Angebote und ein Mangel an grenzüberschreitender Interoperabilität. **Dass beim grenzüberschreitenden Zugang zu öffentlichen Online-Diensten kein höheres Sicherheitsniveau als das einer qualifizierten elektronische Signatur verlangt werden darf, verbessert die Interoperabilität und erleichtert grenzüberschreitende Aktivitäten**: Erstens ist damit die Qualität und Sicherheit des Vertrauensdienstes gewahrt, zweitens sinkt die Unsicherheit der Nutzer über die Gültigkeit der elektronischen Signatur im EU-Ausland und drittens steigen die Anreize für die Anbieter, grenzüberschreitend anwendbare Signaturverfahren zu entwickeln.

Juristische Bewertung

Kompetenz

Die Verordnung wird zu Recht auf Art. 114 AEUV (Rechtsangleichung im Binnenmarkt) gestützt. Dies gilt auch für die Bestimmungen über die elektronische Identifizierung, die eine gegenseitige Anerkennung vorsehen. Denn diese wahrt die Autonomie der Mitgliedstaaten in einem höheren Maße als eine Voll- oder Teilangleichung.

Subsidiarität

Unproblematisch.

Verhältnismäßigkeit

Zur Gewährleistung eines einheitlichen Sicherheitsniveaus der Vertrauensdienste ist der Erlass einer Verordnung verhältnismäßig.

Vereinbarkeit mit EU-Recht

Unproblematisch.

Vereinbarkeit mit deutschem Recht

Das Signaturgesetz schafft die Rahmenbedingungen für elektronische Signaturen. Das Formanpassungsgesetz enthält ihre materiellrechtliche Anerkennung. Aufgrund dieses Gesetzes wurden u.a. das Bürgerliche Gesetzbuch und die Zivilprozessordnung geändert. Die Vorschriften über den elektronischen Identitätsnachweis finden sich im Personalausweisgesetz. Zwar gilt die Verordnung unmittelbar in jedem Mitgliedstaat (Art. 288 UAbs. 2 S. 2 AEUV), d. h. es sind keine nationalen Umsetzungsakte erforderlich. Um die Rechtslage klarzustellen, ist das deutsche Recht jedoch entsprechend anzupassen.

Bislang ungeklärt ist, wie die Mitgliedstaaten die Voraussetzung für die Notifzierung erfüllen können, dass die zur Identifizierung erforderlichen Daten eindeutig einer Person zugeordnet sein müssen. In Betracht kommen die Zuteilung einer Personenkennziffer, die Verwendung der Seriennummer des Identifizierungsmittels oder die Kombination unterschiedlicher Merkmale wie Name, Geburtsname, Adresse. Dabei ist das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) zu wahren. Es darf nur im „überwiegenden Allgemeininteresse" eingeschränkt werden [1 BvR 209/83 u.a. (Volkszählung)].

Zusammenfassung der Bewertung

Die grenzüberschreitende Anerkennung und Akzeptierung elektronischer Identifizierungsmittel kann Bürokratie- und Transaktionskosten senken. Der Verzicht auf eine Prüfung, ob die Identifizierungssysteme die Anforderungen der Verordnung und Mindestsicherheitsstandards erfüllen, erleichtert den Missbrauch und gefährdet die Sicherheit von Personendaten. Die Aufsichtsregeln für die Anbieter der – besonders sensiblen – qualifizierten Vertrauensdienste sind unpräzise und inkonsistent. Die Vorschriften zur Sicherheit elektronischer Signaturen verbessern die Interoperabilität, was grenzüberschreitende Aktivitäten erleichtert.